UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF (1) A HP ENVY 17 NOTEBOOK COMPUTER AND (2) A HP HPSD320A EXTERNAL HARD DRIVE CURRENTLY IN THE CUSTODY OF U.S. PROBATION, 55 PLEASANT STREET, CONCORD, NH, AND (3) A BLACK ONN USB FLASH DRIVE CURRENTLY IN THE CUSTODY OF MERRIMACK COUNTY DEPARTMENT OF CORRECTIONS, 314 DANIEL WEBSTER HIGHWAY, BOSCAWEN, NH	)))))))))))

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Derek Dunn, a Special Agent with Homeland Security Investigations (HSI), being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant authorizing the search of (1) a Hewlett Packard (HP) Envy 17 Notebook computer and (2) a Hewlett Packard HPSD320A external hard drive seized from Gregert Johnson (JOHNSON) by U.S. Probation & Pretrial Services (USPPS) and currently in USPPS custody at 55 Pleasant Street, Concord, New Hampshire and (3) a black Onn USB Flash Drive seized from JOHNSON by Merrimack County Department of Corrections (MCDOC) and currently in MCDOC's custody at 314 Daniel Webster Highway, Boscawen, New Hampshire (hereinafter collectively referred to as THE DEVICES). I seek authority to seize and search THE DEVICES and extract from them electronically stored information that constitutes evidence, fruits, and instrumentalities of

criminal violations which relate to the possession of child pornography, as described in Attachment B.

2. I am a Special Agent with the Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations, and have been so employed since April 2003. I am currently assigned to the Manchester, New Hampshire field office. As part of my regular duties as an agent, I investigate criminal violations relating to a broad range of immigration and customs related statutes, including those relating to child exploitation and child pornography. I have received training in the area of child pornography and child exploitation, and as part of my duties have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media, including digital/computer media. I have conducted investigations and executed search warrants involving child exploitation and child pornography offenses.

3. I am a "Federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant.

4. The information contained in this affidavit is based on information conveyed to me by other law enforcement officials. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have set forth all material information but have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of the Specified Federal Offenses are presently located on the devices.

5. I submit that the facts set forth in this affidavit establish probable cause to

believe that violations of 18 U.S.C. § 2252A(a)(5)(B) (possession of child pornography) have been committed by JOHNSON and that there is probable cause to believe that evidence and fruits, and instrumentalities of violations of that crime, as set forth below, will be found on THE DEVICES.

STATUTORY AUTHORITY

6. This application is part of an investigation into JOHNSON for the alleged knowing possession of child pornography. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing any child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

7. "Child pornography" includes any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct where (A) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (B) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (C) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. 18 U.S.C. § 2256(8).

8. "Sexually explicit conduct" is defined by 18 U.S.C. § 2256(2)(A) as "actual or simulated (i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal . . .; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition

of the genitals or pubic area of any person."

9. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, legally obscene or that do not necessarily depict minors in sexually explicit conduct.

10. "Minor" means any person under the age of 18 years. 18 U.S.C. § 2256(1).

11. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image; and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format. 18 U.S.C. § 2256(5).

PROBABLE CAUSE

12. On March 18, 2025, Supervisory U.S Probation Officer, Scott Davidson of the USPPS in the District of New Hampshire, provided your affiant with the following information.

13. On September 12, 2016, the Court sentenced JOHNSON on a charge of Possession of Child Pornography. The Court imposed a 36-month term of imprisonment and lifetime supervised release.

14. On May 13, 2019, JOHNSON was released from the Bureau of Prisons and commenced his term of supervised release.

15. JOHNSON's special conditions of supervision included conditions that he: (1) "neither possess nor have under his control any material depicting sexually explicit conduct as that term is defined in 18 U.S.C. § 2256(2) involving adults or children"; (2) "is barred from the use of the internet and all media devices with interactive computer service . . . without the prior approval of the probation officer; and (3) "shall consent to and cooperate with unannounced examinations of any computer owned or controlled by the defendant."

16. On April 18, 2023, the probation office submitted a Request for Summons and Modification of the Conditions or Term of Supervision. That document requested that the Court add the following special conditions of supervised release:

a) You must not go to, or remain at, any place where you know children under the age of 18 are likely to be, including parks, playgrounds, and childcare facilities.

b) You must not go to, or remain at, a place for the primary purpose of observing or contacting children under the age of 18.

17. On May 22, 2023, JOHNSON appeared before the Court pursuant to the Summons. At that hearing, JOHNSON consented to the modifications and the Court ordered the imposition of the above noted conditions.

18. On October 4, 2024, a probation officer met with JOHNSON at JOHNSON's residence. JOHNSON presented a National Geographic Outdoor Recreation Mapping Software DVD and requested to use his computer to install it. After confirming the software did not require an internet connection, the probation officer approved its use solely for that purpose. The probation officer verified JOHNSON did not have internet access at his residence and reiterated that he is not to access the internet on his computer. JOHNSON agreed.

19. On January 24, 2025, a probation officer met with JOHNSON at JOHNSON's residence. During that meeting, the probation officer requested to examine JOHNSON's computer (specifically, a HP Envy 17 Notebook computer) to ensure he had not accessed the internet. JOHNSON consented and during the examination, the probation officer discovered an internet browser history that contained the words "Brunette show nice bi firm tits." Again, JOHNSON's conditions of supervision prohibited him from accessing the internet or possessing

any pornography.

20. When asked if he watched pornography, JOHNSON admitted he watched pornography. JOHNSON stated the pornography was on an external hard drive (specifically, a HP HPSD320A external hard drive), which he provided to the probation officer. The probation officer asked JOHNSON if he had accessed the internet, to which JOHNSON replied he had not and reiterated he only viewed pornography stored on the external hard drive. The probation officer seized JOHNSON's HP Envy 17 Notebook computer and HP HPSD320a external hard drive.

21. That same day, the probation officer and Supervisory U.S. Probation Officer Scott Davidson conducted a preliminary review of JOHNSON's computer. No images were immediately seen, but Google, Chrome and Firefox internet browsers contained history with descriptions consistent with pornography. A review of the computer indicated the network/internet capabilities were disabled.

22. On January 30, 2025, a probation officer shipped the aforementioned computer and external hard drive to the Western District of North Carolina's Cyber Lab for analysis. On February 3, 2025, the Western District of North Carolina's Cyber Lab received JOHNSON's computer and hard drive.

23. On February 13, 2025, a probation officer completed a Petition for Warrant or Summons for Offender Under Supervision, citing three violations of supervised release.

24. On February 14, 2025, a probation officer received a summary of the contents recovered from JOHNSON's computer and external hard drive. According to the examiner's report, suspected child sexual abuse material (CSAM), was located on both devices. For example, there were several sub-folders with hundreds of images of young girls modeling in

swimsuits, dance costumes, and regular clothing; there were several pornographic images mixed with pictures of young females wearing dance clothing or swimwear attire. There were also four collages of child erotica images, nude females, and suspected CSAM. Specifically, one of the images appears to be a prepubescent girl, with pigtail braids, performing oral sex on an erect penis.

25. On March 6, 2025, a probation officer completed a Superseding Petition for Warrant or Summons for Offender Under Supervision, to include an additional violation based upon contents that were recovered from JOHNSON's computer and external hard drive. This warrant was approved and signed by U.S Magistrate Judge Talesha Saint-Marc.

26. On March 8, 2025, JOHNSON was arrested pursuant to the above warrant and transported to the Merrimack County Department of Corrections (MCDOC) for booking. While in the processing area, a MCDOC officer conducted a pat search of JOHNSON and recovered several items, including a brown leather eyeglasses case. Inside the case were a pair of glasses, a white cleaning cloth, and wrapped up within the cleaning cloth was a black Onn USB flash drive. An examination of the contents on that flash drive has not been conducted.

27. I know from my training and experience that given the prohibited nature of child pornography, individuals possessing child pornography often take steps to conceal their possession.

28. The computer and external hard drive are currently stored at USPPS at 55 Pleasant Street, Concord, New Hampshire. The flash drive is currently stored at MCDOC at 314 Daniel Webster Highway, Boscawen, New Hampshire. In my training and experience, I know that THE DEVICES have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when THE DEVICES

first came into the possession of USPPS and MCDOC.

TECHNICAL TERMS

29. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

30. Based on my training, experience, and research, I know that THE DEVICES have capabilities that allow them to store data. The HP computer in particular has capabilities that allow it to potentially access the Internet and download items from the Internet. In my training and experience, examining data stored on devices of these types can uncover, among other things, evidence that reveals or suggests who possessed or used the devices.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

31. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

32. There is probable cause to believe that things that were once stored on THE DEVICES, particularly the HP computer, can still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

33. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how THE DEVICES were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on THE DEVICES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information

on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

34. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

35. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

36. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of THE DEVICES described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

/s/ Derek Dunn
Special Agent Derek Dunn
Department of Homeland Security
Homeland Security Investigations

Subscribed and sworn to before me
on April 9, 2025
Apr 10, 2025

UNITED STATES MAGISTRATE JUDGE
Andrea K. Johnstone

ATTACHMENT A

The property to be seized and searched includes the following:

1) a Hewlett Packard Envy 17 Notebook computer seized by U.S. Probation & Pretrial Services (USPPS) from Gregert Johnson on January 24, 2025 and currently in the custody of USPPS, 55 Pleasant Street, Concord, NH,

2) a Hewlett Packard HPSD320a external hard drive seized by USPPS from Gregert Johnson on January 24, 2025 and currently in the custody of USPPS, 55 Pleasant Street, Concord, NH, and

3) a black Onn USB flash drive seized by Merrimack County Department of Corrections (MCDOC) from Gregert Johnson on March 8, 2025 and currently in the custody of MCDOC, 314 Daniel Webster Highway, Boscawen, NH

This warrant authorizes the seizure and forensic examination of the above devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

All records on the devices described in Attachment A that relate to violations of 18 U.S.C. § 2252A(a)(5)(B) (possession of child pornography) and involving Gregert Johnson since May 13, 2019, including:

1) In any format and medium, all originals, computer files, and copies of child pornography as defined in 18 U.S.C. § 2256(8), child exploitation material, visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), images or videos of children showering or using the bathroom, or child erotica.

2) Any and all documents, records, or correspondence, in any format or medium (including, but not limited to, e-mail messages, chat logs, electronic messages, and other digital data files), pertaining to use or ownership of the Devices described in Attachment A.

3) Any and all documents, notes, and any other records that relate to the sexual abuse or exploitation of children or that are reflective of a sexual interest in children.

4) Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

5) Records evidencing the use of Internet protocol addresses to access child exploitation websites, including:

    a. Records of Internet protocol addresses used; and

    b. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.